

INTEGRASI NIST 800-30, RISK IT, DAN COBIT 2019 DALAM PERANCANGAN MITIGASI RISIKO INFRASTRUKTUR TI DI BANK ABC

R. Budiraharjo ^{1)*}, Reneta Elza ²⁾, Riskika Marditia ³⁾, Fatimah Azzarah ⁴⁾,
Fatimah Aulia Aliyah⁵⁾

^{1,2,3,4,5)}Program Studi Sistem Informasi, Institut Teknologi Nasional,
Jl. PKH Mustafa no. 23, Bandung 40124, Indonesia

*Corresponding Author: budiraharjo@itenas.ac.id

ABSTRAK

Perkembangan pesat sektor perbankan meningkatkan risiko TI yang kompleks. Penelitian ini menganalisis peran Komite Pengarah Teknologi Informasi (ITSC) dalam mengurangi risiko di Bank ABC Indonesia dengan mengintegrasikan NIST SP 800-30, Risk IT, dan COBIT 2019. Data dikumpulkan melalui kuesioner kepada pemangku kepentingan untuk mengidentifikasi 30 potensi risiko TI yang dikategorikan berdasarkan proses bisnis, teknologi, manusia, dan lingkungan. Analisis menemukan 12 ancaman signifikan yang dipetakan dalam skenario risiko untuk mitigasi yang lebih efektif. Hasil penelitian menunjukkan bahwa meskipun Bank ABC memiliki infrastruktur TI yang kuat, ancaman siber dan kerentanan operasional tetap menjadi tantangan. Untuk mengatasi ini, dikembangkan model penilaian risiko yang mengintegrasikan faktor risiko spesifik organisasi ke dalam Manajemen Risiko Keamanan Informasi (ISRM). Model ini membantu meningkatkan ketersediaan, kerahasiaan, dan integritas sistem informasi, serta menyelaraskan strategi TI dengan tujuan bisnis. Kesimpulannya, pendekatan proaktif terhadap manajemen risiko TI sangat penting untuk menjaga ketahanan operasional dan kepercayaan pelanggan dalam lingkungan perbankan digital yang terus berkembang.

Kata kunci: *Manajemen Risiko TI, NIST SP 800-30, Risk IT, COBIT 2019, Integrasi Kerangka Kerja.*

1. PENDAHULUAN

Sektor perbankan telah berevolusi selama berabad-abad, dimulai dari praktik kuno seperti pinjaman dan transaksi keuangan. Seiring dengan perkembangan sosial dan teknologi, perbankan telah beradaptasi, dengan tonggak sejarah seperti pendirian bank pertama dan penerapan praktik terstandar. Institusi perbankan secara historis menunjukkan ketangguhan dan fleksibilitas dalam merespons perubahan lanskap ekonomi dan kebutuhan pelanggan (Hanson, 2024). Integrasi teknologi canggih memungkinkan bank untuk meningkatkan efisiensi operasional dan pengalaman pelanggan. Penelitian menunjukkan bahwa teknologi perbankan digital dan finansial telah mentransformasi proses perbankan tradisional (McKinsey & Company, 2024). Di Indonesia, bank regional seperti Bank ABC telah mengadopsi teknologi seperti Smart Mobile Banking, Loan Management System (LMS), dan Cloud Computing untuk memenuhi kebutuhan pelanggan sekaligus meningkatkan efisiensi dan keamanan (Sutherland, 2023).

Namun, ketergantungan pada teknologi juga membawa risiko, termasuk gangguan operasional, ancaman siber, dan kerentanan sistem. Untuk mengatasi

tantangan ini, Bank ABC membentuk Komite Pengarah Teknologi Informasi (ITSC) yang bertugas mengawasi infrastruktur teknologi serta menyusun kebijakan strategis TI. ITSC bekerja sama dengan departemen seperti Keamanan TI, Operasi TI, dan Pengembangan TI untuk menjaga stabilitas dan menyelaraskan strategi teknologi dengan tujuan bisnis bank (Hanson, 2024). Meskipun upaya ini telah dilakukan, diperlukan pendekatan yang lebih komprehensif dalam Manajemen Risiko Teknologi Informasi (ITRM) untuk melindungi layanan dan mempertahankan kepercayaan pelanggan. Implementasi kerangka kerja Manajemen Risiko Keamanan Informasi (ISRM) yang mencakup identifikasi, mitigasi, dan pemantauan risiko menjadi krusial untuk meningkatkan ketahanan siber dan meminimalkan risiko operasional (Asari, 2023).

Salah satu studi di PT Bank BRI mengevaluasi implementasi COBIT 2019 pada proses EDM03 (Ensure Risk Optimization) dan APO12 (Manage Risk) untuk mengukur efektivitas manajemen risiko TI. Hasil penelitian menunjukkan bahwa penerapan COBIT 2019 memungkinkan bank untuk melakukan evaluasi risiko secara komprehensif serta merancang strategi mitigasi yang efektif guna menjaga operasional dan keberlanjutan bisnis (Irawan, K., Hanggara, B. T., & Suprpto, 2023).

Penelitian ini bertujuan untuk menganalisis profil organisasi Bank ABC, dengan fokus pada peran ITSC dalam menyelaraskan strategi teknologi dengan tujuan bisnis. Kajian ini juga mengeksplorasi inisiatif TI utama, seperti Kartu Kredit Indonesia (KKI), Smart Mobile Banking, dan Sistem Deteksi Penipuan (FDS). Penelitian ini diharapkan dapat memberikan kontribusi yang signifikan bagi Bank ABC dalam mengelola risiko TI secara lebih efektif, memastikan ketahanan operasional, dan mencapai tujuan strategis dalam lanskap keuangan yang kompetitif. Selain itu, penelitian ini juga dapat memberikan wawasan berharga bagi industri perbankan secara umum dalam menghadapi tantangan manajemen risiko TI di era digital.

2. METODE

Untuk merancang Dokumen Pedoman Manajemen Risiko yang efektif bagi Bank ABC, kami mengintegrasikan tiga kerangka kerja, yaitu NIST SP 800-30, Risk IT, dan COBIT 2019.

2.1 Kerangka Manajemen Risiko TI

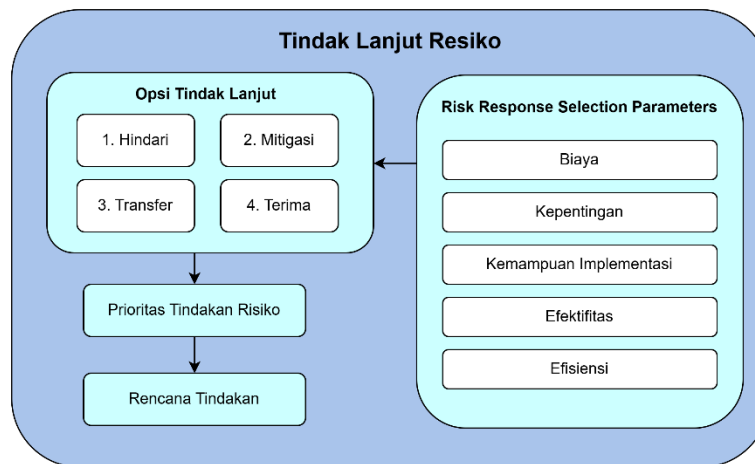
NIST SP 800-30 mengorganisir strategi manajemen risiko dalam lima tugas utama: Identifikasi, Perlindungan, Deteksi, Tanggapan, dan Pemulihan, yang menekankan pentingnya memahami tujuan perusahaan dan toleransi risiko guna mengembangkan program keamanan siber yang sesuai dengan kebutuhan hukum dan operasional (NIST, 2021). Sementara itu, Risk IT Framework yang dikembangkan oleh ISACA berfokus pada identifikasi, evaluasi, dan pengelolaan risiko TI melalui tiga domain utama: Tata Kelola Risiko, Evaluasi Risiko, dan Tanggapan Risiko, yang secara bersama-sama membantu organisasi meningkatkan ketahanan TI melalui strategi mitigasi (Dube & Mohanty, 2020). COBIT 2019, di sisi lain, menyediakan kerangka kerja yang komprehensif untuk tata kelola dan manajemen TI dengan mengintegrasikan kewajiban hukum dan perkembangan teknologi, serta menekankan ruang lingkup manajemen risiko dalam domain APO dan kontrol dalam domain DSS dan BAI untuk memastikan keberlanjutan bisnis (Irawan, 2023).

2.2 Integrasi Kerangka Kerja

Untuk rekomendasi mitigasi, arsitektur ISRM di Bank ABC akan mengintegrasikan COBIT 2019, Risk IT, dan NIST 800-30. Proses ini dimulai dengan penentuan konteks, yang mencakup identifikasi batasan eksternal dan internal dari desain ISRM. Selanjutnya, tahap evaluasi risiko dilakukan berdasarkan pedoman NIST dan Risk IT, yang mencakup identifikasi risiko, pengembangan skenario risiko, dan penilaian ancaman risiko.

Penelitian ini akan difokuskan pada tahap terakhir, yaitu pengembangan rencana tindak lanjut risiko. Setelah identifikasi risiko dan pengembangan skenario, asesmen risiko dilakukan untuk menilai dampak (impact) dan kemungkinan (likelihood) dari ancaman yang telah diidentifikasi. Penilaian ini memungkinkan perankingan risiko berdasarkan prioritas, sehingga risiko dengan prioritas tertinggi dan terendah dapat diidentifikasi. Ancaman-ancaman risiko kemudian dipetakan dalam matriks risiko, yang menunjukkan posisi ancaman terhadap toleransi risiko yang telah disepakati, berdasarkan hasil kuesioner dengan para pemangku kepentingan. Matriks ini mencerminkan area toleransi risiko di Bank ABC, memudahkan identifikasi risiko yang dapat dijadikan peluang, risiko dalam batas toleransi, serta risiko yang melebihi batas toleransi dan memerlukan tindakan mitigasi.

Langkah terakhir adalah pengembangan rencana tindak lanjut risiko, yang mengacu pada COBIT 2019 dan pemilihan opsi tindak lanjut risiko berdasarkan Risk IT 2019. Gambar 1 menggambarkan alur penelitian untuk pengembangan rencana tindak lanjut risiko.



Gambar 1. Alur Penelitian Tindak Lanjut Risiko

2.3 Teknik Pengumpulan Data

Data dalam penelitian ini dikumpulkan melalui penyebaran kuesioner, yang memungkinkan pengumpulan data kuantitatif dari berbagai pemangku kepentingan di lingkungan Bank ABC, sehingga menghasilkan gambaran yang lebih lengkap mengenai analisis kebutuhan pengelolaan risiko infrastruktur TI di Bank ABC.

2.4. Analisis Data

Untuk menentukan risiko yang cukup signifikan untuk dimasukkan ke dalam model Manajemen Risiko Teknologi Informasi, dilakukan proses penilaian terhadap setiap risiko. Penilaian ini mengukur tingkat signifikansi risiko pada skala 1 hingga 4, di mana 1 berarti "tidak penting" dan 4 berarti "sangat penting". Rata-rata skor untuk setiap risiko dihitung guna mengidentifikasi risiko dengan tingkat kepentingan yang kritis. Untuk memperoleh rata-rata skor dari setiap pertanyaan risiko ($\bar{R}_j$), skor yang

diberikan oleh seluruh responden dijumlahkan, kemudian dibagi dengan total jumlah responden (N). Data yang telah terkumpul kemudian diproses untuk menghitung nilai indeksnya menggunakan persamaan (1) berikut.

$$\bar{R}_j = \frac{\sum_{i=1}^N S_i}{N} \quad (1)$$

Keterangan :

RQ_j = Pertanyaan Risiko j

S_i = Skor yang diberikan oleh responden i untuk RQ_j

N = Jumlah total responden

$\bar{R}_j$ = Skor rata-rata untuk pertanyaan risiko j

Risiko dengan skor rata-rata $\bar{R}_j \geq 3,00$ dipilih untuk dimasukkan lebih lanjut ke dalam model Manajemen Risiko TI. Ambang batas ini memastikan bahwa hanya risiko yang dianggap sangat penting oleh responden yang akan melanjutkan ke tahap berikutnya dalam proses manajemen risiko.

3. HASIL DAN PEMBAHASAN

3.1 Identifikasi Risiko

Berdasarkan kuesioner untuk mengidentifikasi potensi risiko terkait infrastruktur TI, teridentifikasi 30 potensi risiko yang terbagi dalam lima kategori: proses bisnis, teknologi, manusia, kerusakan infrastruktur, dan alam. Kuesioner ini disebarkan kepada pemangku kepentingan di Bank ABC untuk menyaring risiko yang relevan dengan operasional bank. Hasilnya, ditemukan 12 ancaman risiko yang akan ditindaklanjuti. Daftar risiko ini mengadopsi standar NIST SP 800-30 dan Risk IT, dengan pengkategorian risiko non-adversarial (NR) dan adversarial (AR) sesuai prinsip NIST. Tabel 1 menjelaskan daftar potensi risiko yang terpilih sebagai ancaman.

Tabel 1. Faktor Penyebab Risiko dan Ancaman Risiko

Faktor Risiko		Ancaman Risiko	
a	Proses Bisnis	NR01	Risiko manajemen TI
		NR02	Ketidaksesuaian antara operasi TI dengan operasi sehari-hari
b	Teknologi	NR03	Risiko dari penerapan teknologi baru
		NR04	Kerusakan perangkat lunak dan data
		AR01	Risiko serangan siber
		NR08	Kerusakan perangkat keras TI
		NR05	Risiko pemadaman listrik
		NR06	Peralatan TI yang sudah usang
		AR02	Serangan malware
c	Manusia	NR07	Kesalahan dalam operasi TI
d	Kerusakan Infrastruktur	NR09	Kerusakan akibat kebakaran pada peralatan TI
e	Alam	NR10	Kerusakan infrastruktur TI akibat bencana alam

3.2 Tindak Lanjut Risiko

3.2.1 Pemilihan Opsi dan Prioritisasi Tindakan Risiko

Dalam pengelolaan risiko infrastruktur TI, kerangka kerja Risk IT menawarkan empat opsi tindakan: menghindari risiko, mengurangi atau memitigasi risiko, memindahkan risiko, dan menerima risiko. Penting untuk mempertimbangkan lima kriteria utama dalam memilih opsi tersebut: biaya tindakan, tingkat kepentingan risiko, kemampuan organisasi dalam implementasi, efektivitas tindakan, dan efisiensi tindakan. Dalam penelitian ini, opsi dan prioritas tindakan risiko ditentukan dengan menyebarkan kuesioner kepada para pemangku kepentingan di Bank ABC. Dari 12 ancaman risiko yang teridentifikasi, sebanyak 10 risiko dipilih untuk ditangani melalui tindakan mitigasi, yaitu NR01 hingga NR08 dan AR01 hingga AR02. Sementara itu, untuk tindakan pemindahan risiko, terdapat 2 ancaman risiko yang diidentifikasi, yaitu NR09 dan NR10.

3.2.2 Strategi Pengurangan Nilai Risiko dan Rencana Tindak Lanjut

Penelitian ini menggunakan COBIT 2019 untuk mitigasi risiko infrastruktur TI di Bank ABC. Risiko yang telah dievaluasi dan diprioritaskan diatasi dengan opsi mitigasi untuk mengurangi dampak atau kemungkinan ancaman, sehingga risikonya turun di bawah batas toleransi. Pemetaan ancaman risiko ke dalam tujuan proses COBIT 2019 dilakukan dengan mencocokkan ancaman dengan kategori risiko COBIT. Penelitian ini berfokus pada domain COBIT terkait pengelolaan operasional (*low level*), dengan pemilihan domain berdasarkan keterhubungan antara ancaman dan aktivitas COBIT. Tabel 2 menjelaskan hasil pemetaan ancaman risiko yang telah ditentukan untuk dimitigasi terhadap *domain* COBIT 2019.

Tujuan utama dari mitigasi risiko adalah mengurangi nilai risiko. Berdasarkan wawancara dan diskusi dengan para pemangku kepentingan, implementasi mitigasi risiko infrastruktur TI di Bank ABC hanya akan menargetkan aktivitas-aktivitas pada COBIT 2019 dengan kapabilitas Tingkat 2. Penetapan ini dilakukan karena Bank ABC belum memiliki kemampuan dan sumber daya yang cukup untuk menerapkan aktivitas COBIT 2019 di atas Tingkat 2. Rancangan strategi mitigasi risiko menggunakan aktivitas Tingkat 2 dari COBIT 2019 kemudian diaplikasikan untuk simulasi asesmen ulang terhadap ancaman risiko terkait. Hasilnya menunjukkan bahwa nilai risiko dari ancaman infrastruktur TI dapat berkurang hingga di bawah batas toleransi risiko yang ditetapkan, sehingga tujuan mitigasi risiko di Bank ABC dapat tercapai. Tabel 2 menyajikan simulasi pengurangan nilai risiko infrastruktur TI di Bank ABC, dengan keterangan "I" untuk dampak (impact) dan "L" untuk kemungkinan (likelihood).

Tabel 2. Simulasi Pengurangan Nilai Risiko

RENCANA MITIGASI						PENGURANGAN RISIKO		
Kode Risiko	I Score	L Score	Nilai Risiko	Target Tingkat Kapabilitas	Aktivitas COBIT 2019	Nilai I Baru	Nilai L Baru	Nilai Risiko Baru
AR01	8	8	64	2	DSS02.02, DSS02.03, DSS02.04, DSS02.05, DSS02.06, DSS02.07, DSS04.01, DSS04.02, DSS04.03, DSS04.04,	8	2	16

AR02	8	8	64		DSS04.06, DSS04.07, DSS05.01, DSS05.02, DSS05.03, DSS05.04, DSS05.05, DSS05.06, DSS05.07	8	2	16
NR01	5	5	25	2	DSS05.01, DSS05.02, DSS05.03, DSS05.04, DSS05.05, DSS05.06, DSS05.07, DSS06.01, DSS06.02, DSS06.03, DSS06.04, DSS06.05, DSS06.06	5	2	10
NR02	5	5	25	2	APO03.01	5	2	10
NR03	8	8	64	2	DSS03.01, DSS03.03, DSS03.04	8	2	16
NR04	5	5	25	2	BAI01.01, BAI01.02, BAI01.04, BAI11.01, BAI11.02, BAI11.04, BAI11.05, BAI11.06, BAI11.07, BAI11.08, BAI11.09	5	2	10
NR05	8	5	40	2	APO06.01, APO06.02, APO06.03, APO06.05	8	2	16
NR06	5	5	25	2	APO05.01, APO05.02	5	2	10
NR07	5	5	25	2	APO07.01, APO07.02, APO07.03, APO07.04, APO07.05, APO07.06	5	2	10
NR08	5	5	25	2	DSS01.01, DSS01.03, DSS01.04, DSS01.05	5	2	10
NR09	8	5	40	TRANSFER RISK		2	5	10
NR10	8	8	64	TRANSFER RISK		2	8	16

4. KESIMPULAN

Penilaian, identifikasi, dan pencegahan risiko yang mengancam ketersediaan, kerahasiaan, dan integritas sistem informasi merupakan tugas penting dalam manajemen risiko keamanan informasi (ISRM). Dengan menerapkan kerangka kerja yang terintegrasi menggunakan NIST 800-30, Risk IT, dan COBIT 2019, Bank ABC dapat mengelola risiko dan melindungi infrastruktur TI mereka. Bank ABC secara proaktif menangani potensi ancaman melalui penilaian risiko, pembuatan skenario, dan respon yang sesuai, sambil memastikan keselarasan sistem dengan tujuan perusahaan dan toleransi risiko.

Kerangka ISRM mencakup definisi ruang lingkup, penilaian risiko, dan pemilihan respon. Proses manajemen risiko diperkuat dan disesuaikan dengan tujuan strategis untuk memastikan ketahanan jangka panjang dengan mengintegrasikan faktor risiko internal dan eksternal. Bank ABC menangani semua risiko berdasarkan penilaian yang mendalam, dengan fokus pada mitigasi prioritas tinggi, melalui pemetaan risiko ke kategori COBIT 2019 dan penyesuaian rencana mitigasi sesuai kebutuhan.

DAFTAR PUSTAKA

- Asari, S. (2023). *Implementasi kerangka kerja ISRM dalam meningkatkan ketahanan siber di sektor perbankan*. Jurnal Keamanan Sistem Informasi, 15(2), 45-60.
- Dube, S., & Mohanty, P. (2020). *Risk governance and risk management frameworks in organizations: A comprehensive review*. Journal of Information Technology Management, 19(3), 112-125.
- Hanson, R. (2024). *Transformasi sektor perbankan melalui teknologi: Perkembangan dan tantangan di masa depan*. Jurnal Ekonomi dan Bisnis, 12(4), 99-115.
- Irawan, H. (2023). *COBIT 2019 dalam pengelolaan risiko TI di sektor perbankan*. Jurnal Manajemen Teknologi, 22(1), 34-50.
- Irawan, K., Hanggara, B. T., & Suprpto. (2023). Evaluasi Tata Kelola dan Manajemen Risiko Teknologi Informasi menggunakan Framework COBIT 2019 proses EDM03 dan APO12 (Studi Kasus pada PT Bank BRI Unit Bangorejo). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 7(5), 2642-2651.
- McKinsey & Company. (2024). *Digital banking and financial technology: The transformation of traditional banking processes*. Retrieved from <https://www.mckinsey.com>
- NIST. (2021). *Cybersecurity framework (CSF)*. National Institute of Standards and Technology. Retrieved from <https://www.nist.gov/cybersecurity-framework>
- Sutherland, D. (2023). *Smart mobile banking and cloud computing: Strategies for financial institutions*. Journal of Banking Technology, 18(2), 134-150.